kraken INTELLIGENCE
ORDO AB CRYPTO

Crypto Yields - Deep Dive on DeFi

February 2021

Table of Contents

1.

Introduction

The Decentralized Finance (DeFi) space has been all the craze this year, with an estimated value of over $11B locked in the DeFi lending market alone.[1] It's likely that you've seen new DeFi platforms with impressive annual percentage yields (APY) advertised for different cryptocurrencies listed on these platforms. Depositing your crypto for a high return can be an appealing offer especially in today's world of negative interest rates and fiat debasement. The generous rates DeFi offers relative to traditional yield-bearing instruments is enticing, but we believe there are significant implied and realized risk premia worth considering. While we intend to outline the risks specific to decentralized lending platforms in this note, we hope it serves as a useful guide for navigating DeFi as the broader ecosystem continues to innovate and disrupt the existing financial industry.

2.

Currency Risk

As we've outlined in our introductory note, the risk-free rate for fiat is pretty straightforward when compared to cryptocurrencies as government bond yields are generally used as the benchmark. In the case of crypto, more specifically stablecoins that are pegged to fiat, we argue the risk-free rate follows that of the pegged fiat. For example, USD-pegged stablecoin USDC would have a risk-free rate of 0.5% if the risk-free rate for USD is 0.5%. Say the interest rate for USDC deposits is 1% on Compound, then the 0.5% spread[2] would be the risk premium. As we've covered before, interest rates are largely a function of the risk-free rate of a "risk-free" investment and the default risk (counterparty risk) associated with lending to a counterparty. This 0.5% would represent the default risk, or risk factors tied to the mechanisms of DAI, such as scenarios of the whole system de-pegging from the USD, or risks pertaining to its collateralized asset ETH, and additional counterparty risks of the lending platform itself.

To illustrate, let's use DAI as an example. DAI is pegged to the USD but backed by ether (ETH), meaning the risk-free rate of DAI will follow the quoted currency through which it was acquired. Assuming we deposit ETH for DAI, the rate for DAI would follow ether's hurdle rate of 4.30% (also ether's current inflation rate, which we will explain in the following paragraph). For non-Proof-of-Stake (PoS) currencies, such as bitcoin, we argue that the risk-free rate is zero. Conversely, in the case of cryptocurrencies with borrowing and issuance tied together as part of their network consensus mechanism, there may be a risk-free rate that accrues to those who lend the currency to the issuing network. This may be the case for ERC-20 tokens like ether in the future, as it moves onto PoS with the launch of Ethereum 2.0.

In the case of ether (ETH), the annual issuance cap is 18M ETH.[3] As of writing, a block is mined roughly every 15 seconds, and the miner is awarded 2 ETH per block mined. With a capped annual issuance, relative dilution decreases annually as more total ether is in

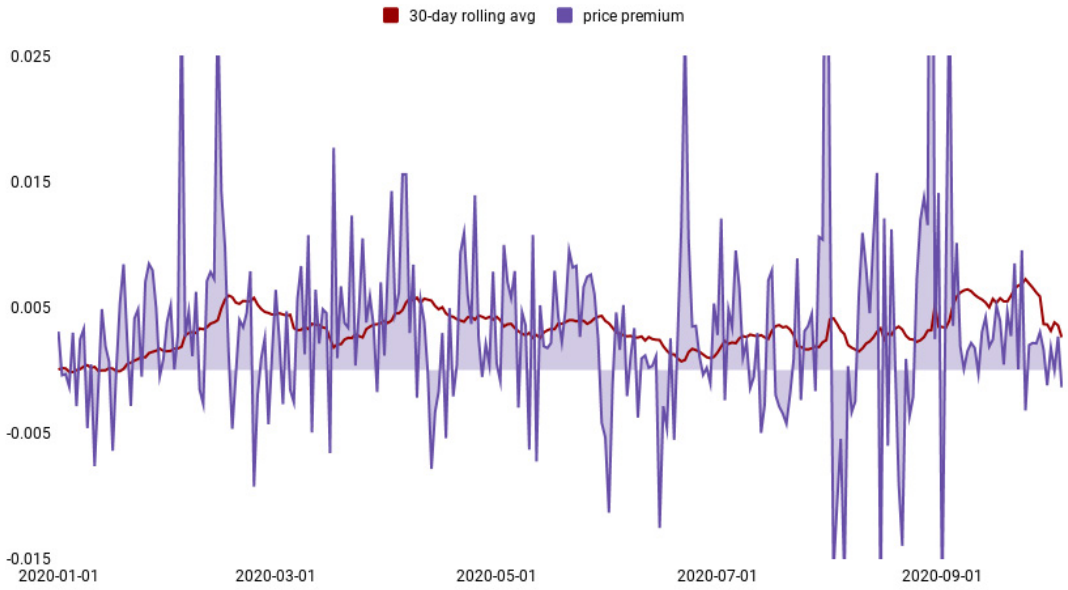
circulation, and the supply growth rate tends towards zero over time. As of writing, the estimated current circulating ether supply is around 114M ETH[4] with an estimated 4.30% annual supply increase. Though we assume ETH has a risk-free rate of 0% like bitcoin, we will consider this dilution rate the hurdle rate of the ETH protocol to compensate for the loss of purchasing power due to inflation.

As most DeFi platforms are currently built on the ethereum network, lending/borrowing is carried out not only in ERC-20 tokens like ETH but also in wrapped tokens, such as Wrapped BTC (WBTC) or Ren BTC (REN). Both are ERC-20 tokens claiming to be backed 1:1 by bitcoin. In a similar vein to USD-backed stablecoins, we argue that BTC-backed tokens will follow the risk-free rate of bitcoin (0%) with an additional counterparty risk. Taking WBTC as an example, WBTC has registered minters of the token, which means the benchmark rate for WBTC would be 0% plus the counterparty risk of minters. There are two main actors in the WBTC ecosystem, namely custodians and merchants. Custodians hold the native asset (BTC) and mint the WBTC tokens. Merchants are the ones to initiate the minting of WBTCs to custodians, and the ones who directly interact with users looking to receive WBTCs. Merchants are also the ones to burn WBTC tokens, which is the act of redeeming BTC for existing WBTC tokens.[5] Both merchants and custodians must be registered and verified parties, which reduces the counterparty risk of WBTC to these designated partners. Though this is an example of risk in the custodial element of a token, understanding the mechanism of token creation can allow us to identify the existing risks for a cryptocurrency.

As an example, to quantify the counterparty risk of WBTC, we can look at the historical price difference between WBTC and BTC, as we believe the difference indicates market pricing of the risk associated with WBTC. This price divergence can show us the spread attributable to the counterparty risk of minters of the currency at a given time. In figure 1, we look at the difference between the two protocol's closing prices. As of writing, though the spread ranged from -1.9% to 6.9% this year, the 30-day average spread was 0.24%, which we will use as the risk premium of WBTC protocol.

Figure 1

WBTC price premium to BTC, YTD



Source: Coinmarketcap

Overall, there will be varying degrees of risk-free rates or none depending on the crypto asset, and for those with none, interest rates will be a function of risks unique to each currency, platform, and therefore the yield product.

3.

Platform Risk

Though demand for lending (and borrowing) can come in various forms within the realm of DeFi, we will focus on two types of platforms - DeFi lending and Automated Market Makers (AMMs), to make it conceptually more comparable with traditional yield-bearing products. As we know, DeFi is an open financial system that operates within a decentralized, peer-to-peer, and code-based system. In this context, DeFi lending is the decentralized and more private version of a traditional yield-bearing product where you receive interest on each currency deposited, and AMMs are essentially liquidity aggregator platforms that match orders from a pool of tokens.

Figure 2

DeFi lending and AMM platforms and respective yields

Lending Platform/Annual Yield	WBTC	ETH	DAI
Aave	0.19%	0.13%	3.86%
Compound	0.06%	0.05%	3.06%
dYdX	-	0.02%	8.74%
Fulcrum	8.74%	1.33%	8.74%
Oasis Savings/Dai Savings Rate (DSR)	0.00%		

AMM Platform/Annual Yield	REN	USDT	SBTC
Curve	2.78%	5.90%	1.28%
	Top 3 liquidity pools		
Balancer	15% - 80%		
Uniswap	Liquidity providers receive a transfer fee from people conducting exchanges. The exchangers are charged 0.3% which is split amongst all liquidity providers of the specific pool based on the proportion of liquidity they're offering in the pool.		

Source: Aave, Oasis, Balancer, Curve, Defirate.com, Uniswap
Note: APY rates at time of writing. Please note that yield rates are subject to change at any given time.

Before delving into the risks present on these platforms, we will incorporate what we've noted about currency risk in the section above. As an example, we look at the various yields offered for DAI deposits on different lending platforms. We can deduce the implied risk of each platform by subtracting the risk premium of DAI (in this case, the hurdle rate of ETH) to get an approximate rate of counterparty risk attributable to each lending platform.

Figure3

Currency risk and implied risk by lending platform

Lending Platform	DAI supply APY =	DAI risk premium	+ Implied platform risk premia
Aave	3.86%	4.30%	-0.44%
Compound	3.06%		-1.24%
dYdX	8.74%		4.44%
Fulcrum	8.74%		4.44%

Source: Aave, Compound, dYdX, Fulcrum
Note: APY rates at time of writing. Please note that yield rates are subject to change at any given time.

Similarly for WBTC, if we assume a 0.24% risk premium, we can deduce the risk of various platforms as follows:

Lending Platform	WBTC supply APY =	WBTC risk premium	+ Implied platform risk premia
Aave	0.19%	0.24%	-0.05%
Compound	0.06%		-0.18%
Fulcrum	8.74%		8.50%

Source: Aave, Compound, Fulcrum
Note: APY rates at time of writing. Please note that yield rates are subject to change at any given time.

Though these are simplistic examples, it shows us a way to break down variability of risk for different assets and DeFi applications.

Then what are the risks present in these DeFi lending and Automatic Market Maker (AMM) platforms? Though each platform has its own set of participants and mix of assets, for a general understanding, we will use a couple of major players that exist in the DeFi market today to illustrate some of the common risks present in the space.

Smart contract risk

One main risk associated with DeFi applications is the risk of protocol exploitation through bugs or errors in its smart contracts. In 2020, multiple lending and AMM platforms experienced exploitations that resulted in up to millions in locked funds drained.[6,7,8] Faulty codes or bugs can be manipulated by attackers to target networks and platforms. As human written code is prone to errors, both participants and lending platforms must find better ways to manage the level of risk on their platforms. Proactive security and code audits as well as verifications are now conducted by some platforms to manage this risk across its protocol's smart contracts. Not only active exploitation attempts, but also the case of unexpected protocol failures can be a source of financial risk to all participants involved.

To illustrate, there has been roughly $86M lost from DeFi exploitations in 2020.[9] This impacted value accounts for around 0.58% of the estimated $14.7B total value locked in DeFi during the same period of time.[10] Though anecdotal, this 0.58% can represent a default loss from smart contract risks. Exploitations increased this year with the rise of DeFi, which means that unlike some traditional financial products that are insured to protect consumers, many DeFi platforms may not yet have proper coverage or insurance measures in place that guarantee fund safety. Until the industry progresses and platforms find ways to incorporate better security validation measures, individuals should exercise more caution with solutions like Nexus Mutual that insure against specific smart contracts and risk events.

One of the reasons for smart contract exploitations is due to oracles. As blockchains cannot interact with data from external systems, oracles communicate real-time data to smart contracts as an intermediary. This creates a potential attack vector where

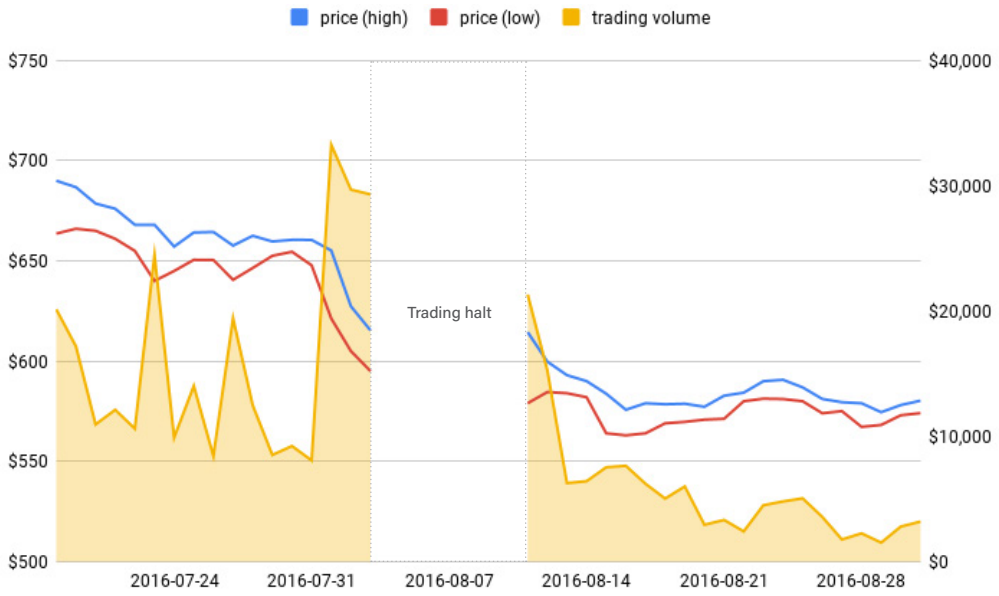
malicious actors can take advantage of poorly designed oracles to control the information sent out to smart contracts and hijack the outcome. Many DeFi applications run on centralized oracles, where independent sources will report data without coordinating with other sources to check the authenticity of that data. This creates a single point of failure and creates room for greater counterparty risk. For example, a yield farming protocol reported a loss of $6M in Nov. 2020, after an attacker exploited its centralized price oracle.[11] Though there are currently multiple projects focused on mitigating these risks and creating decentralized solutions to oracles, the oracle problem remains.

Counterparty risk

If we assume the likelihood of a protocol being exploited is 0.58%, then how do we quantify the level of trust people place on said riskier platforms at a given period in time? One way is to compare the prices of an asset on two or more platforms to measure the level of trust placed on the counterparty. As per figure 4, we look at the bitcoin price on Bitfinex during its August 2016 distributed denial-of-service (DDoS) attack.

Figure 4

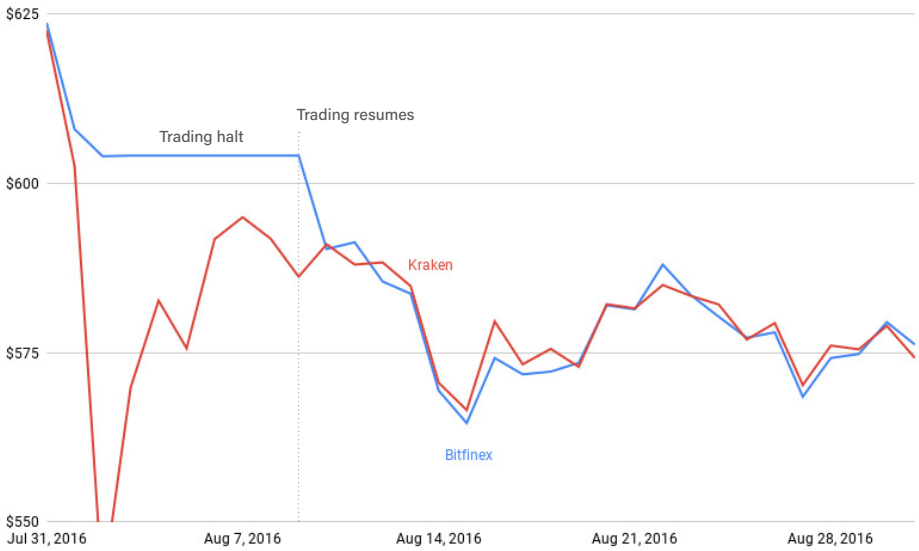
Bitcoin price on Bitfinex during August 2016 DDoS attack



Source: Cryptowatch

Figure 5

Bitcoin price difference on Kraken vs. Bitfinex the day trading resumes on Bitfinex



Source: Cryptowatch

As shown in figures 4 and 5, after roughly 120K BTC was stolen from Bitfinex on August 2nd, bitcoin prices began to fall and Bitfinex halted trading activities for the next couple of days.[12] Per figure 4, trading volumes slowed on Bitfinex despite falling prices as participants tried exiting the platform. In figure 5, we compared the price of bitcoin on Bitfinex and Kraken during the hacking event. On the day of the hack, prices closed with a 11.8% difference, with a spread range of 0.6% - 28.4%. This range is what we identify as the risk premium of using the platform during that specific time of uncertainty.

Liquidity and collateralization risk

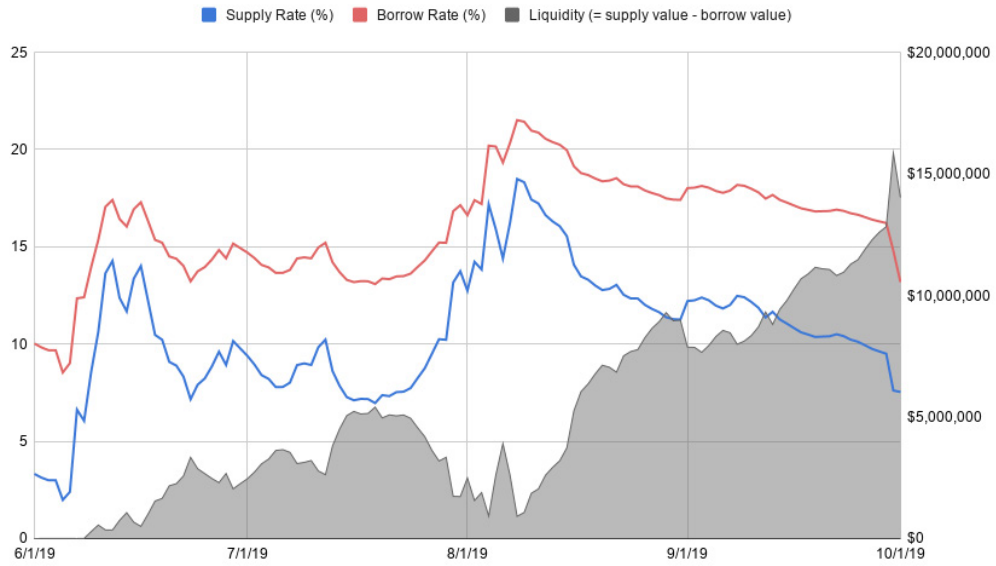
DeFi lending will only be as diversified as its sources of liquidity. Robust AMMs and lending platforms will be those that offer liquidity from a wide set of participants with uncorrelated behavior, ensuring less risk of liquidity evaporating during times of

crises. At the moment, most DeFi loans are over-collateralized to counteract illiquidity and credit risk. To be prepared for possible scenarios where a lender won't be able to exit a position or access their funds whenever they wish, platforms specify collateral instruments, collateralization ratios, and cap the borrowing/withdrawals at the size of the liquidity pools. Thus, the average liquidity and make up of collateral assets available on a protocol can be another indicator of risk.

In managing fluctuations in liquidity, some platforms will set dynamic interest rates. For instance, on Compound, during times of low supply-side liquidity, both token supply and borrowing APRs[13] will increase to incentivize participants to supply more liquidity and for borrowers to repay their borrowed tokens. Conversely, the APR for supplying and borrowing tokens will decrease in times of high supply-side liquidity to incentivize participants to take out cheaper loans. In this way, platforms can manage their exposure to the risk of illiquidity.

Figure 6

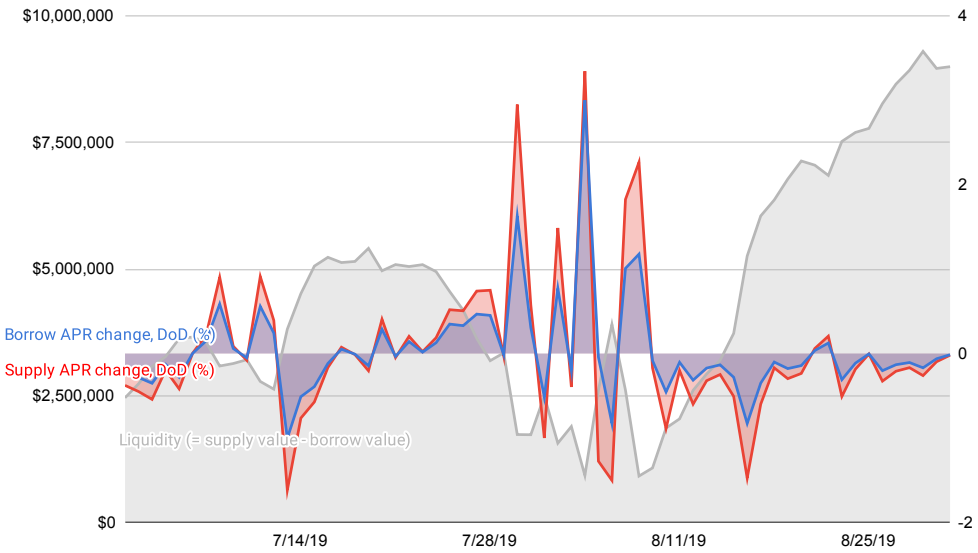
Liquidity vs. APRs in Compound's SAI market



Source: Compound

Figure 7

Borrow and supply APR day-on-day change (%), Compound's SAI market



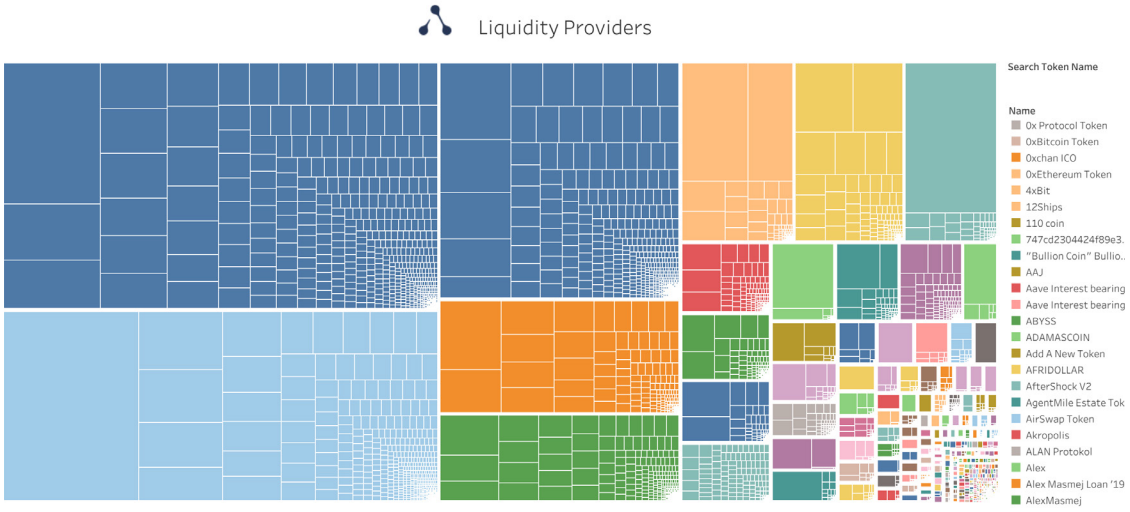
Source: Compound

Per figure 7, low liquidity events trigger an increase in both borrow and supply APRs, which results in a surge of liquidity available on the platform. For example, between 6 - 8 August 2019, liquidity fell by over 76% on Compound's SAI market, which caused supply and borrow APRs to rise by 4% and 2%, respectively. Liquidity surged by 17% the following day and continued to rise. In this market, we see that there were 3 near-illiquid events in 2H2019, where APRs adjusted within a range of 0.6%-3.3% on supply rates and within a range of 0.4%-3.0% on borrow rates, leading to a rise in liquidity the next day. Though it's hard to predict when illiquidity will occur on a platform, looking back at its historical events and analyzing how markets reacted can help us understand the risks involved in participating in that particular market or venue.

Another indicator of risk could be in the makeup of liquidity providers in liquidity pools. Pools heavily concentrated in a few large providers could subject other participants to risk in the event that these individuals pull out and ignite a cascade of withdrawals. Looking to figure 8, we see the makeup of liquidity providers on Uniswap, with some assets heavily concentrated to a handful of large liquidity providers.

Figure 8

Liquidity providers by asset on Uniswap



Source: Alethio
Note: Each square represents one provider.

Some other platforms like the MakerDAO have emergency settlement mechanisms in place to avoid potential market collapse.[14] Whichever the venue, looking for platforms that actively prepare for events of possible illiquidity or "bank" runs will be important in mitigating risk.

Governance risk

As a platform's rules and the general development of a protocol are impacted by its governance structure, there is a risk that said governance negatively impacts the platform. Applications that do not have an open governance structure place admin capabilities in the hands of a centralized few, meaning there can be changes made to the protocol without the consideration of a majority of participants involved. As a user, keeping up with these upgrades is another task that can leave room for risk if not carried out in a timely manner.

Maker is an example of an open governance platform, where holders of the MKR token govern the system through votes. Holders of the token can vote on all important changes to the platform. Similarly, Compound has also changed its structure to an open governance model where the COMP token holder community and their delegates will be the ones to propose and vote on any proposed protocol changes. It's set up in a way that any accepted changes by the majority of the community will be implemented after a two day grace period. Open governance can take different forms, but the central purpose is to take a decentralized approach to a protocol's growth and security.

Though it's difficult to quantify the risk of governance, either as it changes to an open or closed structure, we look to the Maker protocol as an example to gauge market sentiment towards open governance changes. The Maker Foundation transferred control of the MKR token to the Maker governance community on Dec. 20, 2019.[15] This was a step towards decentralization as MKR token holders were given full control, with decentralized governance being the only way to change MKR token authorizations. Prices of MKR reacted to this change by rising 3.1% from $490 on Dec. 19 to $505 by Dec. 21, 2019.

Similarly, the Synthetix Foundation stepped down as the central party guiding the direction of the Synthetix protocol on July 29, 2020. This was an attempt to move towards a more community-owned and decentralized governance structure where 3 decentralized autonomous organizations (DAOs) would take control of the protocol and be led by the wider community and token holders. The price of the network token (SNX) reacted to this change by rising 8.7% the next day. Though it would be misleading to conclude that open

governance protocols hold less risk than centralized governance, it's important to note that fully understanding the governance structure of each protocol, as well as knowing historical market reactions to governance-related changes on the protocol, can be an indicator of possible risks present on a platform.

Liquidity pool risk

Automated Market Makers (AMMs) are slightly different in that they are decentralized exchanges that operate through the interaction of smart contracts. Traditional functions of an exchange such as trade execution and settlement are carried out by smart contracts and these simplistic trading functions come together to operate liquidity pools. Liquidity pools have pairs of assets that will be mixed to form a pool of tokens from which people can deposit and exchange. For instance, if there is a USDT/ETH 50/50 pool, this liquidity pool will have a set total pool token value, which means the proportion of the trading pairs (USDT & ETH) in a pool will fluctuate to keep the total value constant with every trade made in the pool. The 50/50 also means that any liquidity provider wishing to participate in the pool must provide an equal value of both USDT and ETH to the pool.

Under this structure, there is a risk present in some Automated Market Makers (AMMs) known as impermanent loss. In the case of a price discrepancy between exchanges, arbitrageurs will buy tokens for cheaper in a pool until prices go up in the pool and there is no longer an opportunity for profit. This transaction leaves the liquidity providers (LPs) with an unrealized loss, given the pool will have an increase in the asset that is depreciating and decrease in the asset that is appreciating. This loss is said to be "impermanent" until their liquidity is withdrawn from the pool, at which point the loss would be permanent. However there are other factors that must be considered when determining net profit/loss, such as transaction fees awarded to LPs and mining rewards for providing liquidity or using a protocol, which could offset the value lost by "impermanent" permanent losses.[16]

One way to theoretically measure this risk with a given currency in a liquidity pool is by defining a price range of ±3 standard deviations from the asset's 20-day simple moving average price.[17] Liquidity providers can use this measure of volatility as a reference point

for the potential loss that could occur on any particular day. For ease of understanding, assume ETH/USDT is currently trading at 100 USDT with a 20-day average of 90 USDT with an upper limit of 105 USDT. This upper band signifies over 99% likelihood of price moving as high as 105 USDT intra-day.

Now assume a liquidity provider places 1 ETH and 100 USDT into a Uniswap USDT market with 100 ETH and 10,000 USDT. The provider will have a 1% stake in a liquidity pool with an implied price of 1 ETH = 100 USDT,[18] where the product of the two liquidity pools stays constant. Say the price fluctuates and hits the upper price limit of 105 USDT (per 1 ETH). As the total liquidity stays constant, a fluctuation in price can change the size of each token's liquidity pool and consequently the value of a provider's stake in the pool. The new value of the liquidity provider's 1% stake in the ETH pool comes to 0.97 ETH and 1% in the USDT liquidity pool comes to 102.4 USDT. When converted to USDT, this is a total of 204.94 USDT.[19] Had the individual held onto the 1 ETH and 100 USDT, the total stake would have come to 205 USDT,[20] translating into a loss of 0.06 USDT (or 0.0000011% loss) before factoring in any additional fees given out from the pool.

To minimize this risk, some exchanges have liquidity pools that only contain assets of similar value, usually in the form of stablecoins. Pools that hold stablecoins or tokens of relatively stable value minimize the risk of impermanent loss as tokens tend to be less volatile in relation to one another. Another way of negating some of this risk is to participate in liquidity pools with various token weights outside the standard 50/50 weighted pool model. This way LPs can choose the level of exposure they have to different assets. Most recently, another model of minimizing this risk was introduced through the use of price oracles that feed external prices into the pools for automatic adjustment. Whichever platform you choose to use, understanding the construct of these decentralized exchanges/AMMs is important in managing your risk.

As these examples illustrate, the level of risk on DeFi can be measured in different time frames or around specific events. In figure 9, we consolidate all mentioned risks and the implied risk rates to get a better understanding of the market pricing of each of the risks based on our examples. Please note that these risk rates are based on very specific events

in set points in time, and are only meant to illustrate a way of finding implied DeFi hurdle rates. They are by no means a permanent or definite measure of the current risk present on the platforms mentioned. Just as crypto interest rates are subject to fluctuations at any given time, so are most risk rates.

Figure 9

Implied platform risk rates

Risks	Implied risk rates	Average
Smart contract risk	0.58%	0.58%
Counterparty risk	0.63% ~ 28.46%	14.54%
Liquidity risk (APR risk)	0.40% ~ 3.30%	1.85%
Governance risk	3.09% ~ 8.74%	5.92%
Liquidity pool risk	0.0000011%	0.0000011%
Implied hurdle rate	**4.7% ~ 40.5%**	**22.9%**

Note: The risks rates listed are merely anecdotal and based on specific scenarios on chosen platforms, and not meant to be taken as definitive figures of each risk.

Though there is more than one way to quantify risk, or trust in DeFi, having a benchmark rate to which you can extrapolate layers of risk will be helpful in understanding that depositing in DeFi ≠ depositing in a bank.

4.

Conclusion

DeFi has opened up access to financial services for both banked and unbanked individuals globally through the use of the internet. With new participants joining in and traditional banks failing to offer appealing rates, people are turning to opportunities that not only offer a generous return but also allow participation in popular financial products that cross geographical boundaries. Knowing this, we hope to educate market participants in the DeFi space while also encouraging individuals to be more security-aware and risk-cognizant. The world of cryptocurrencies is still vastly different from traditional systems and its offerings, but once we understand the risks associated with these new platforms and applications, we believe that we can make informed decisions and manage the risks that affect the yield of DeFi investments. Between the inherent complexities of DeFi and the value Kraken places on security, we hope that a better understanding of DeFi and its risks will improve overall security standards across this industry as market participants make informed decisions and demand greater platform security.

Footnotes

1. DeFi Total Value Locked (TVL) as of January 2021. DeFi Pulse (https://defipulse.com)
2. The difference between the return on a risky asset and the risk-free rate
3. Not inclusive of ETH rewards for uncle blocks
4. "All the Ether you can trade" Kraken Futures (https://blog.cfbenchmarks.com/all-the-ether-you-can-trade/)
5. WBTC Network (https://wbtc.network/)
6. "'Sophisticated' Hacker Plunders $450,000 From Defi Protocol Balancer" Bitcoin.com (https://news.bitcoin.com/sophisticated-hacker-plunders-450000-from-defi-protocol-balancer/)
7. "The DeFi Hack: What Decentralized Finance Should and Shouldn't Be" Andrew Rossow (https://cointelegraph.com/news/the-defi-hack-what-decentralized-finance-should-and-shouldnt-be)
8. "DeFi Lender bZx Loses $8M in Third Attack This Year" Paddy Baker (https://www.coindesk.com/defi-lender-bzx-third-attack)
9. "Crypto-in-Review 2020: The Year of the Bull" Kraken Intelligence (https://kraken.docsend.com/view/f5yrdazcjw6n3955)
10. Total Value Locked (USD) in DeFi from 1 January 2020 to 31 Dec 2020. (https://defipulse.com/)
11. "After $6 Million Hack, Value DeFi Turns to Chainlink for Help" Decrypt (https://decrypt.co/48892/value-defi-hacked-chainlink)
12. "Bitcoin Drops Nearly 20% as Exchange Hack Amplifies Price Decline" Charles Bovaird (https://www.coindesk.com/bitcoin-drops-12-exchange-hack-amplifies-price-decline)
13. Annual percentage rate
14. Maker Protocol Emergency Shutdown Mechanism (https://docs.makerdao.com/smart-contract-modules/shutdown)
15. "The Transfer of MKR Token Control: A Giant Leap Toward System Decentralization" Maker Blog (https://blog.makerdao.com/transfer-of-mkr-token-control-a-giant-leap-toward-system-decentralization/)
16. In other words, unrealized loss.
17. Bollinger bands; ±3 standard deviations from the average statistically offer a 99.7% confidence that the price will likely trade within the price range.
18. ETH price = USDT liquidity pool / ETH liquidity pool (https://pintail.medium.com/uniswap-a-good-deal-for-liquidity-providers-104c0b6816f2)
19. 0.97 ETH + 102.4USDT = 102.4 USDT + 102.4 USDT = 204.94 USDT
20. 1 ETH + 100 USDT = 105 USDT + 100 USDT = 205 USDT

We appreciate your feedback! Please visit https://surveys.kraken.com/jfe/form/SV_805WrOgbowxvHff to participate in a brief survey. For all future Kraken Intelligence content, sign up here. For comments, suggestions, or questions related to this article or future topics you'd like to learn more about, you may also direct your communication to intel@kraken.com or to your account manager.

Kraken provides access to 54 cryptocurrencies spanning more than 250 markets with advanced trading features, industryleading security, and on-demand client service. With the acquisition of Crypto Facilities, Kraken now offers seamless access to regulated derivatives on 5 cryptocurrencies with up to 50x leverage. Sign up for a free account in minutes at www.kraken.com/sign-up. We look forward to welcoming you.

For multi-exchange charting, trading, portfolio tracking, and high resolution historical data, please visit https://cryptowat.ch. Create a free Cryptowatch account today at https://cryptowat.ch/account/create and enjoy a 14 day trial of premium service.

For OTC-related execution services or inquiries, please direct your communication to otc@kraken.com or to your account manager.

Disclaimer